

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

### Listing of Claims:

---

B17

1           1. (Currently amended) A method for facilitating access to a plurality of  
2 applications that require passwords, comprising:  
3           receiving a request for a password from an application running on a  
4 remote computer system, the request being received at a local computer system;  
5           authenticating the request as originating from a trusted source, wherein  
6 authenticating the request involves authenticating the remote computer system  
7 that sent the request;  
8           using an identifier for the application to look up the password for the  
9 application in a password store containing a plurality of passwords associated with  
10 the plurality of applications, wherein the plurality of passwords allows a different  
11 password to be used with each application of the plurality of applications; and  
12           if the password exists in the password store, sending the password or a  
13 function of the password to the application on the remote computer system.

1           2. (Original) The method of claim 1, wherein the request for the password  
2 includes computer code that when run on the local computer system requests the  
3 password on behalf of the application on the remote computer system.

1           3. (Currently amended) The method of claim 2, wherein the computer code  
2 is in the form of a platform-independent JAVA-applet that runs on a platform-  
3 independent JAVA-virtual machine on the local computer system.

1           4. (Currently amended) The method of claim 3, wherein sending the  
2 password or the function of the password to the application to the remote  
3 computer system involves:  
4           communicating the password to the platform-independent JAVA-applet;  
5 and  
6           allowing the platform-independent JAVA-applet to forward the password  
7 to the application on the remote computer system.

1           5. (Currently amended) The method of claim 3, wherein the platform-  
2 independent JAVA-applet is a signed platform-independent JAVA-applet, and  
3 wherein authenticating the request includes authenticating the platform-  
4 independent JAVA-applet's certificate chain.

1           6. (Original) The method of claim 1, wherein authenticating the request  
2 involves authenticating a creator of the request.

1           7. (Canceled).

1           8. (Original) The method of claim 1, further comprising, if the password  
2 store is being accessed for the first time,  
3           prompting a user for a single sign on password for the password store; and  
4           using the single sign on password to open the password store.

1           9. (Original) The method of claim 8, wherein if a time out period for the  
2 password store expires,  
3           prompting the user again for the single sign on password for the password  
4 store; and  
5           using the single sign on password to open the password store.

1           10. (Currently amended) The method of claim 1, wherein if the password  
2 store is being accessed for the first time, the method further comprises  
3 authenticating the user through an authentication mechanism, wherein the  
4 authentication mechanism includes one of~~can include~~:  
5           a smart card;  
6           a biometric authentication mechanism; and  
7           a public key infrastructure.

1           11. (Original) The method of claim 1, wherein if the password does not  
2 exist in the password store, the method further comprises:  
3           adding the password to the password store; and  
4           sending the password to the application on the remote computer system.

B17  
1           12. (Original) The method of claim 11, wherein adding the password to the  
2 password store further comprises automatically generating the password.

1           13. (Original) The method of claim 11, wherein adding the password to the  
2 password store further comprises asking a user to provide the password.

1           14. (Original) The method of claim 1, further comprising decrypting data  
2 in the password store prior to looking up the password in the password store.

1           15. (Original) The method of claim 1, wherein the password store is  
2 located on a second remote computer system.

1           16. (Previously presented) The method of claim 1, wherein the password  
2 store is located on one of:  
3           a local smart card;

4 a removable storage medium; and  
5 a memory button.

1 17. (Original) The method of claim 1, further comprising:  
2 receiving a request to change the password from the application on the  
3 remote computer system;  
4 automatically generating a replacement password;  
5 storing the replacement password in the password store; and  
6 forwarding the replacement password or the password function to the  
7 application on the remote computer system.

B<sup>17</sup>  
1 18. (Currently amended) A computer-readable storage medium storing  
2 instructions that when executed by a computer cause the computer to perform a  
3 method for facilitating access to a plurality of applications that require passwords,  
4 the method comprising:  
5 receiving a request for a password from an application running on a  
6 remote computer system, the request being received at a local computer system;  
7 authenticating the request as originating from a trusted source, wherein  
8 authenticating the request involves authenticating the remote computer system  
9 that sent the request;  
10 using an identifier for the application to look up the password for the  
11 application in a password store containing a plurality of passwords associated with  
12 the plurality of applications, wherein the plurality of passwords allows a different  
13 password to be used with each application of the plurality of applications; and  
14 if the password exists in the password store, sending the password or a  
15 function of the password to the application on the remote computer system.

1           19. (Original) The computer-readable storage medium of claim 18,  
2 wherein the request for the password includes computer code that when run on the  
3 local computer system requests the password on behalf of the application on the  
4 remote computer system.

1           20. (Currently amended) The computer-readable storage medium of claim  
2 | 19, wherein the computer code is in the form of a platform-independent JAVA  
3 | applet that runs on a platform-independent JAVA-virtual machine on the local  
4 computer system.

B<sup>17</sup>  
1           21. (Currently amended) The computer-readable storage medium of claim  
2 20, wherein sending the password or the function of the password to the  
3 application to the remote computer system involves:  
4 |           communicating the password to the platform-independent JAVA-applet;  
5 and  
6 |           allowing the platform-independent JAVA-applet to forward the password  
7 to the application on the remote computer system.

1           22. (Currently amended) The computer-readable storage medium of claim  
2 | 20, wherein the platform-independent JAVA-applet is a signed platform-  
3 | independent JAVA-applet, and wherein authenticating the request includes  
4 authenticating the platform-independent JAVA-applet's certificate chain.

1           23. (Original) The computer-readable storage medium of claim 18,  
2 wherein authenticating the request involves authenticating a creator of the request.

1           24. (Canceled).

1           25. (Original) The computer-readable storage medium of claim 18,  
2 wherein the method further comprises, if the password store is being accessed for  
3 the first time,  
4           prompting a user for a single sign on password for the password store; and  
5           using the single sign on password to open the password store.

1           26. (Original) The computer-readable storage medium of claim 25,  
2 wherein if a time out period for the password store expires, the method further  
3 comprises:  
4           prompting the user again for the single sign on password for the password  
5 store; and  
6           using the single sign on password to open the password store.

B<sup>17</sup>  
1           27. (Currently amended) The computer-readable storage medium of claim  
2 18, wherein if the password store is being accessed for the first time, the method  
3 further comprises authenticating the user through an authentication mechanism,  
4 wherein the authentication mechanism includes one of~~can include~~:  
5           a smart card;  
6           a biometric authentication mechanism; and  
7           a public key infrastructure.

1           28. (Original) The computer-readable storage medium of claim 18,  
2 wherein if the password does not exist in the password store, the method further  
3 comprises:  
4           adding the password to the password store; and  
5           sending the password to the application on the remote computer system.

1           29. (Original) The computer-readable storage medium of claim 28,  
2 wherein adding the password to the password store further comprises  
3 automatically generating the password.

1           30. (Original) The computer-readable storage medium of claim 28,  
2 wherein adding the password to the password store further comprises asking a  
3 user to provide the password.

1           31. (Original) The computer-readable storage medium of claim 18,  
2 wherein the method further comprises decrypting data in the password store prior  
3 to looking up the password in the password store.

B17  
1           32. (Original) The computer-readable storage medium of claim 18,  
2 wherein the password store is located on a second remote computer system.

1           33. (Previously presented) The computer readable storage medium of  
2 claim 18, wherein the password store is located on one of:  
3 a local smart card;  
4 a removable storage medium; and  
5 a memory button.

1           34. (Original) The computer-readable storage medium of claim 18,  
2 wherein the method further comprises:  
3 receiving a request to change the password from the application on the  
4 remote computer system;  
5 automatically generating a replacement password;  
6 storing the replacement password in the password store; and

7 forwarding the replacement password or the password function to the  
8 application on the remote computer system.

1 35. (Currently amended) An apparatus that facilitates accessing a plurality  
2 of applications that require passwords, comprising:

3 a receiving mechanism that receives a request for a password from an  
4 application running on a remote computer system, the request being received at a  
5 local computer system;

6 an authentication mechanism that authenticates the request as originating  
7 from a trusted source, wherein the authentication mechanism is configured to  
8 authenticate the remote computer system that sent the request;

9 a lookup mechanism that uses an identifier for the application to look up  
10 the password for the application in a password store containing a plurality of  
11 passwords associated with the plurality of applications, wherein the plurality of  
12 passwords allows a different password to be used with each application of the  
13 plurality of applications; and

14 a forwarding mechanism that sends the password to the application on the  
15 remote computer system if the password exists in the password store.

1 36. (Original) The apparatus of claim 35, wherein the request for the  
2 password includes computer code that when run on the local computer system  
3 requests the password on behalf of the application on the remote computer system.

1 37. (Currently amended) The apparatus of claim 36, wherein the computer  
2 code is in the form of a platform-independent ~~JAVA~~-applet that runs on a  
3 platform-independent ~~JAVA~~-virtual machine on the local computer system.



1           38. (Currently amended) The apparatus of claim 37, wherein the  
2 forwarding mechanism is configured to send the password to the application on  
3 the remote computer system by:  
4           communicating the password to the platform-independent JAVA-applet;  
5 and  
6           allowing the platform-independent JAVA-applet to forward the password  
7 to the application on the remote computer system.

1           39. (Currently amended) The apparatus of claim 37, wherein the platform-  
2 independent JAVA-applet is a signed platform-independent JAVA-applet, and  
3 wherein the authentication mechanism is configured to authenticate a certificate  
4 chain.

17  
B  
1           40. (Original) The apparatus of claim 35, wherein the authentication  
2 mechanism is configured to authenticate a creator of the request.

1           41. (Canceled).

1           42. (Original) The apparatus of claim 35, wherein if the password store is  
2 being accessed for the first time, the lookup mechanism is configured to:  
3           prompt a user for a single sign on password for the password store; and to  
4           use the single sign on password to open the password store.

1           43. (Original) The apparatus of claim 42, wherein if a time out period for  
2 the password store expires, the lookup mechanism is configured to:  
3           prompt the user again for the single sign on password for the password  
4 store; and to  
5           use the single sign on password to open the password store.

1 44. (Currently amended) The apparatus of claim 35, wherein if the  
2 password store is being accessed for the first time, the lookup mechanism is  
3 configured to authenticate the user through an authentication mechanism, wherein  
4 the authentication mechanism includes one of ~~can include~~:

5 a smart card;  
6 a biometric authentication mechanism; and  
7 a public key infrastructure.

1 45. (Original) The apparatus of claim 35, further comprising an insertion  
2 mechanism, wherein if the password does not exist in the password store the  
3 insertion mechanism is configured to:

4 add the password to the password store; and to  
5 send the password to the application on the remote computer system.

1 46. (Original) The apparatus of claim 45, wherein the insertion mechanism  
2 is additionally configured to automatically generate the password.

1 47. (Original) The apparatus of claim 45, wherein the insertion mechanism  
2 is additionally configured to ask a user to provide the password.

1 48. (Original) The apparatus of claim 35, further comprising a decryption  
2 mechanism that is configured to decrypt data in the password store.

1 49. (Original) The apparatus of claim 35, wherein the password store is  
2 located on a second remote computer system.

1 50. (Previously presented) The apparatus of claim 35, wherein the  
2 password store is located on one of:

3 a local smart card;  
4 a removable storage medium; and  
5 a memory button.

1 51. (Original) The apparatus of claim 35, further comprising a password  
2 changing mechanism that is configured to:  
3 receive a request to change the password from the application on the  
4 remote computer system;  
5 automatically generate a replacement password;  
6 store the replacement password in the password store; and to  
7 forward the replacement password to the application on the remote  
8 computer system.

B17  
1 52. (Currently amended) A method for facilitating access to a plurality of  
2 applications that require passwords, comprising:  
3 receiving a request to look up a password at a password server;  
4 authenticating the request as originating from a trusted source, wherein  
5 authenticating the request involves authenticating the remote computer system  
6 that sent the request;  
7 wherein the request is received from a client and includes an identifier for  
8 an application requesting the password from the client;  
9 using the identifier for the application to look up the password for the  
10 application in a password store containing a plurality of passwords associated with  
11 the plurality of applications, wherein the plurality of passwords allows a different  
12 password to be used with each application of the plurality of applications; and  
13 if the password exists in the password store, sending the password or a  
14 function of the password to the client, so that the client can present the password  
15 to the application.

1           53. (Previously presented) The method of claim 52, wherein the request is  
2 received from computer code running on the client that requests the password on  
3 behalf of the application.

1           54. (Currently amended) The method of claim 53, wherein the computer  
2 code is in the form of a platform-independent ~~JAVA~~ applet that runs on a  
3 platform-independent ~~JAVA~~ virtual machine on the client.

B17  
1           55. (Currently amended) A server that distributes code for facilitating  
2 access to a plurality of applications that require passwords, wherein the code  
3 operates by:  
4           receiving a request for a password from an application running on a  
5 remote computer system, the request being received at a local computer system;  
6           authenticating the request as originating from a trusted source, wherein  
7 authenticating the request involves authenticating the remote computer system  
8 that sent the request;  
9           using an identifier for the application to look up the password for the  
10 application in a password store containing a plurality of passwords associated with  
11 the plurality of applications, wherein the plurality of passwords allows a different  
12 password to be used with each application of the plurality of applications; and  
13           if the password exists in the password store, sending the password or a  
14 function of the password to the application on the remote computer system.

---